ISSN 2350-1049

International Journal of Recent Research in Interdisciplinary Sciences (IJRRIS)
Vol. 6, Issue 2, pp: (10-15), Month: April - June 2019, Available at: www.paperpublications.org

The impact of cybersecurity on the future of Autonomous ships

Kazem Said Mahmoud Agamy

International Forum for Maritime Transport

Arab Academy for Science, Technology and Maritime Transport

Abstract: **In the present future, there will be numerous ships steaming the seas split between conventional and Autonomous ships. Both type of ships is operating in various areas of the globe with various degree of security. Due to the novel of the autonomous ships, the effect of cyber security is not clear yet (K. Jones et al, 2016). The principle reasons are the lack of and inability of assessing the risks and the vulnerabilities of autonomous ships (Allianz Global Corporate and Specialty, 2016). The issue of cyber security might be an added value to the autonomous ships and a reason for a fast spreading and might be a derailment factor, this will be determined in the next few years, depending on technology which intended to be used in communication and also in the regulatory frame work, and finally on the amount of awareness and training. This paper aims to predict, in an exploratory approach the risks and vulnerabilities which may affect autonomous ships in case of cyberattacks. To predict cyber risk for autonomous ships sampling the existing cyber risk, the results will not be accurate but might be a base for future researches.**

Keywords: **Cybersecurity - Autonomous ship – Cyberattacks – cyber awareness – Threat scenarios.**

1. INTRODUCTION

The maritime industry with a long history of trading between nations, aiming to a simplified goal of transporting good and human safely from one place to another. The industry has entered a new phase in the last few years. More sophistication came to shipbuilding starting from design and drawing stage till operation. Interlinked with harbors and ways of operation and management. All infrastructure has now become a mixture of electromechanical constructs and highly integrated hardware and software forming a set of computer networks that cover the whole industry and communication with many of its stakeholders (Tucci, 2017). The interlinking between various networking and censoring all over modern ships and computers ashore whether at shipping companies, ports, terminal, shipyard or makers makes ships prime targets and more vulnerable to piracy and terror acts via cyber-attacks. The more the ship becomes digitalized and computerized the more the attacks become prone and advanced.

The impact and the scope of such attacks are variable from one case to the other, the major problem is that the information related to many incidents were not disclosed to public or even reported but was suspected to be occurred as noted by Rothblum ‘a number of maritime cyber incidents have also not been disclosed to the public or misclassified as machine or human error’ (Rothblum 2000). These incidents show how vulnerable ships and shipping related activities such as ports operations are. The understanding of cyber-attacks is not so clear or definitive yet, so defenses are not yet fully preventable. The stealth ability and long attack duration as the case of Barcelona ports, of new cyber attacks increase the number of cyberthreats in general, including maritime cyberthreats (Allianz Global Corporate & Specialty, 2016).

Autonomous ships which are no longer a fiction but a fact and soon will be sailing the seas, are not far from cyber attacks. The threats expected to be more frequent and the magnitude will be higher, but before reaching this conclusion, first what is the cyber-attacker aiming for! it’s a high noon to think to pirate a ship for the sake and the value of the ship itself but; to make certain damage to reputation, disbalance a business or even economy, financial interest or terrorist act.

2. INCIDENTS OF MARITIME CYBER ATTACKS

On 22 June, off the Russian port of Novorossiysk, a master of a ship had reported that his GPS had put him in a position off original position by 32 kilometers inland, actually at Geledzhik airport. All the navigation equipment onboard was working properly, out suspicious the captain have contacted the surrounding ships at least 20 ships were encountering the same effect and all located at the same spot Geledzhik airport (D. Hambling, 2017)

The attack on China Ocean Shipping (COSCO) on various locations at USA, South America, and Canada. Though systems were affected a shore, but none onboard were affected according to media reports, official information was not released. (P. Paganini, 2018) The effected lasted few days. The incident will focus the lights on which link of operation the attack will be liable to be affected or the effects started from. This incident will draw the attention that in case of autonomous ship the attack will be more directed to the RCC, and ca hardly affect or target the ship itself for a simple reason, there will be no crew onboard, the possibility of triggering attach from within shipboard operation will be minor, but the attack can be triggered from shore to ship by the IT system thereafter the attach will pass through IT to essential OT onboard

The ransom ware Petrya affected Maersk Shipping Company on 2017; the attack targeted the operation of containers, tugboats and tankers. The computer network was crippled, the losses mounted up to 300 million USD, the effect send a shockwave on almost all the shipping industry. During the time of attack and recovery of all the operation were performed manually. (D. Palmer, 2017). The problem with this case is that the ransomware has the ability to spread like a worm rapidly infecting every device in the operation.

The attack can be as mentioned earlier in the form of GPS Spoofing. To prove that spoofing is possible, researchers from the Department of Engineering and Engineering Mechanics at the University of Texas at Austin performed a test. The research targeted a Yacht, creating a falsified GPS signal, the researchers succeeded to spoof the GPS receiver and set the yacht off course the test was done by a small spoofing device located 30 miles ashore, the signal was weak at first, then increased gradually to let the GPS receiver to follow the strongest signal as it always do, then sending the wrong signal, resulting on setting the wrong location of the yacht, and though the crew onboard tried to bring the ship to course, but failed and the yacht still following the wrong signal. (B. Brewin, 2013)

The attack in the form of GPS Jamming, though signal jamming is spread all over the world but the most significant was noticed off the cost of South Korea, when over 250 ships were affected, that was back on April 2015 (J. Ryall, 2016). The claim was that this Jamming resulting from a state sponsored actor in North Korea, the problem arises when ships or aircraft in critical situation during land fall or landing, where dense traffic is expected and precise position is needed.

Port were not far from the cyber attacks, the port of Barcelona was a victim of cyberattack, luckily the port administration had a contingency plan for such risks, there is no official report about the attack, the attackers hits several servers but the operation were not interrupted, this attack followed by another attack at the port of San Diego both attacks were a ransomware attack. (J. Johnson, 2018). The director of Europol, Rob Wainwright, says the internet is being used to facilitate the international drug trafficking business. This was following the cyberattack on Belgian port of Antwerp. Luckily the attackers were caught by police in Belgium and Holland. At this case the attack lasted two years started from 2011 till 2013. The organized crime drug traffickers used a hacker group from Belgium to infiltrate computer networks in at least two companies in the port of Antwerp to traffic cocaine and heroin in legitimate cargo of timber and banana from south America.

3. EXAMPLE OF TARGETED EQUIPMENT ONBOARD

All equipment which is connected to networking and internet is prone and subject to cyberattack, for instance:

- Global Positioning System (GPS), and the entire Global Navigation Satellite Signal (GNSS) is prone to be subject to cyberattack, the system is known to have a weak security measure, it can be easily manipulated as will be seen on sampled case next.

- Electronic Chart Display and Information System (ECDIS) is a potential target of cyberattack, as of the case of USS Guardian which was grounded off Philippines. ECDIS, as per the investigation shows the reefs eight miles off location resulting on the grounding, though it was not a cyberattack but it proves that reliance on electronic only with open data access may lead to such an attack.

ISSN 2350-1049

International Journal of Recent Research in Interdisciplinary Sciences (IJRRIS)
Vol. 6, Issue 2, pp: (10-15), Month: April - June 2019, Available at: www.paperpublications.org

- Automatic Identification System (AIS) is prone to spoofing signal, could be used by vessel operator to falsify position or hide location.

- Very Small Aperture Terminal (VAST) with many spreads all over onboard ships can be the first place to have an easy and unprotected access to the ship network.

- Many USB ports onboard which is connected to the network and internet. As shown in Figure 1.

Figure 1: ECDIS keyboard with an unprotected USB input

3. AUTONOMOUS SHIP

Cyberattack on conventional ships were not clearly or official released to public, all reports were released through media reports. This will make the issue even more difficult in relation to Autonomous ship (T.Pilter, 2005).

4. THREAT SCENARIOS

The expected threats which can trigger or affect the cyber security of the autonomous ship can be comprised the following,

- A device can be hooked up to any of the system linked to the network, such as a flask memory stick or similar USB device during building stage, or maintenance sessions.

- A hostile party gets control of the ship through communication link.

- Signal jamming directed to the positioning devices onboard or ship navigation controls i.e. GPS.

- Blocking to the signal between the RCC and the ship.

- Spoofing the GPS signal which is received by the receiver onboard.

To conclude the above threats, an evaluation of sampled threats will be compared between conventional ships and Autonomous ships. Since navigation will be the prime target point to control, misguide a ship, the attackers will target equipment which need to be updated frequently, using USB input, CD/DVD and via internet/satellite, such as AIS, NAVTEX, ECDIS. In case of ECDIS, whether using Raster chart display system or redundant system both can be prime target for cyber attack though with various degree of ease. These cases maybe have less impact to Autonomous ship, since users will not be able to access the ships system via USB or CD/DVD, but through internet. The internet in this case will be accessed through the link to RCC, so the intruder or the attacker will have to hack into the RCC first to get access to the ship.

It is clear that the only access to autonomous ship will be the internet, which will be also the most positive point in comparison to conventional ship, since the shipboard network is the gate way to the internet. Being away from local internet access prevent workstation from hooking up to relatively affordable internet access, making a barrier to workstation software and operation system frequent and regular important updates. These updates are very important to malware and spyware security updates, accordingly the system become more vulnerable to cyber attacks (Simon and Ray 2004). Furthermore, the use of outdated operation system onboard, which sometimes used from the time the ship came into service. These systems sometime are outdated and became obsolete, the maker of the software might have stopped updating these operation systems, in the case of Autonomous ship, all operating system will be updated continuously as it is linked all the time to the RCC, if the RCC OS is updated, by default the systems onboard are updated.

ISSN 2350-1049

International Journal of Recent Research in Interdisciplinary Sciences (IJRRIS)
Vol. 6, Issue 2, pp: (10-15), Month: April - June 2019, Available at: www.paperpublications.org

The most serious and sophisticated factor to cyber security is the human factor, 75% of maritime casualties are related to human factor (Rothblum, 2000). Contrdictury, the most effective way to counteract cyber-attack is through a well-trained and aware crewmember and in the case of autonomous ship an RCC team member. The existence of an angry and not satisfied crew member or a blackmailed crewmember can have an easy access to the ship's system, the access of visitors who need to use ship printers to print documents (BIMCO et al, 2017). Crewmembers proper training and screening for security clearance can be a first step to have a ship secure against cyberattack comprising cyber awareness.

5. CYBER AWARENESS

The more technology brought to ships the more prone to cyber attacks, thence the more internet of things (IoT) the more the ship become closer to Internet of Everything (IoE), as expected in the case of autonomous ship, internet of everything make human interference less, unless well trained personnel this might lead to systems isolation. To reach this stage the transitional period will require proper training for personnel onboard still involved in data entry and access to IT. But once the ship become IoE phase, it will transfer from the weak link in the chain to the most difficult link, attackers will find ship not as a prime target but will look ashore for an easier link to launch the cyber-attack which might or might not affect the ship as cargo, or hull. However, training and monitoring will be the best wall against cyberattack, a company IT security policy and task training will be first step, followed by procedures to prevent free USB ports and devices, a proper password security set on all input devices. According to Survey performed by Futurenautics on 2015, only 12 percent of the crew received any training related to cybersecurity. Selina Singh stated "The greatest vulnerability to any system is normally the user. It is therefore increasingly important to recognize the value of having an informed, trained and responsible workforce when it comes to cyber threats,"

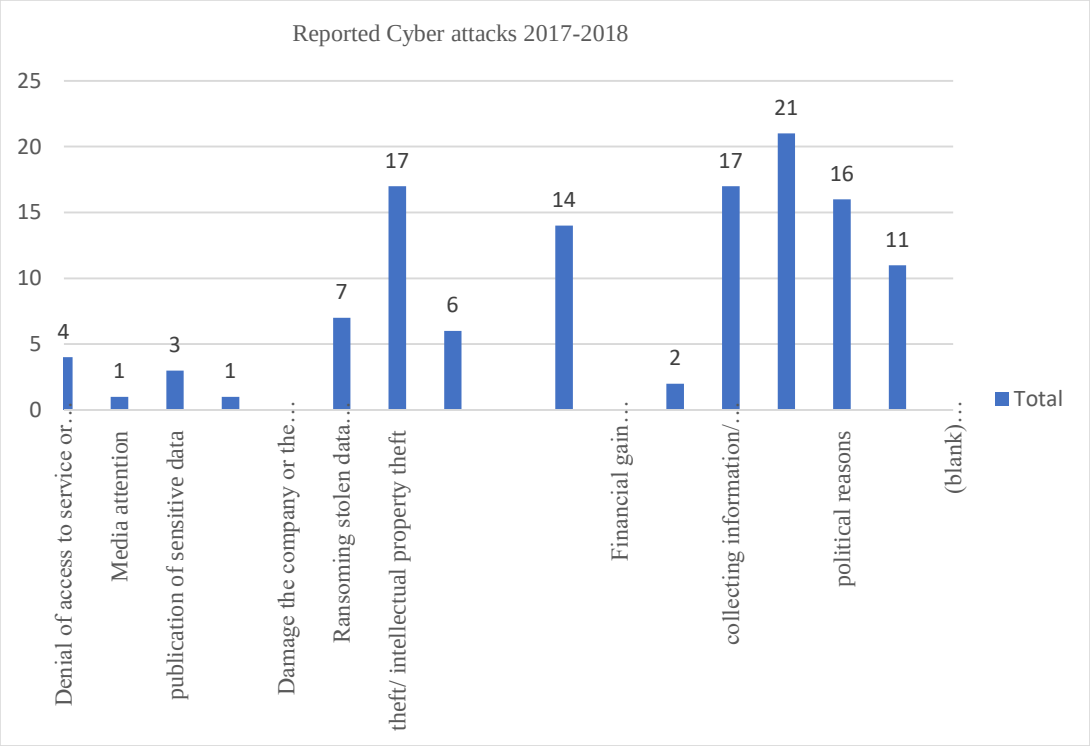

Figure 2: graph of reported Cyberattacks occurred between 2017 and 2018

The data used to structure Figure 2, was collected from raw data issued by Center for Strategic & International Studies. For the year 2017 and 2018. The focus was on cyberattacks on government agencies, defense and high-tech companies and economic crimes, though the ransom ware Petrya affected Maersk Shipping Company on 2017 the losses mounted up to 300 million USD, the attack is an economic crime, but nevertheless it was not mentioned at the report. The majority of the attacks related to espionage and theft of solid money from banking systems or firms. There is no clear or firm information regarding attacks on shipping companies or ship within this report or any other available data. The point here is that every company, firm, or any economic structure trying to protect their image and reputation by shedding information related to cyberattacks resulting on stealing of data, ransom of data or theft of money for economic reasons,

this resulting on lack of information about the attacks, and accordingly crippling the efforts to find the most suitable and effective way to combat any future attacks. This might reduce the cyber awareness within the shipping community, accordingly the need to formulate a clear and unified framework to report, and regulate the action prior and after cyber attack is imminent.

6. FOCUSING THE FRAMEWORK

Internationally, in an attempt to bridge the diversity of approaches to cybersecurity, IMO in 2017 made amendment to International Safety Management Code (ISM) and The International Ship and Port Facility Security Code (ISPS), to detail how risk management process should be implemented and how operators of ports and ships should include cybersecurity as integral part of the process. Making the operators more aware and conscious of the cyber risks. This step is considered as initial action to set a wider set of cybersecurity regulations. However, this step came very late and slowly moving forward, the amendments intended to come into force January 2021, the first autonomous ships which is expected to operate without crew and operated remotely at her first phases, already at testing phases and expected to operate unmanned on 2020, regardless of being operated costal or worldwide still prone to cyberattack without someone onboard to discover, report or intercept any attack.

Nationally, the first governmental attempt in the national level was performed by Australia, where a Defense white paper issued at 2000 considering cyberattacks as a matter of national security, followed by E-security Initiatives which made public on 2008. The Australian Cyber Security Center was established on 2009 and the issuance of the Final Security Strategy was released on 2017 with the purpose of observing the targeted routers with malicious activities.

The General Data Protection Regulation (GDRP) of the EU came in effect on 2018, with other countries in Asia are on the same track. The European Union Council on 2017 asked for the adoption of a common approach to EU cybersecurity. The UK National Security Strategy on 2015 considered cyber threat as a Tier One risk to UK interest, on September 2017, UK on its Cyber Security Code of Practice for ships affirmed that cybersecurity is a mounting concern for global economy including shipping and maritime industry

7. FUTURE COMPLIANCE

The applicability of GDPR requires that each company dealing with personal data either in processing or handling, need to take enough measures to protect these data, failure to do so will result on a huge fine. In maritime industry this means that almost every exporter, importer, operator, owner who will have a direct or indirect link with EU member individuals will need to comply with these GDPR, this means that, all traders have business with EU member has to comply with GDPR, by other words GDPR will be an international and a worldwide regulation, the question will be how to regulate and imply fines if any. Furthermore, how regulate the time frame within which the reporting and action needed to be implemented. If for instance the breach affected data of crewmembers outside the EU, how the Privacy Impact Assessments will be performed. To a data protection officer in a small company operating with multinational crew will be a heavy burden on owners and operators, even for ISM and ISPS compliance, since this step should be done following proper training for personnel on how to handle personal data protection both onboard and ashore.

The UK Government announced that critical services companies dealing with energy, transportation, water and health can be fined up to 17 million pounds if they fail to demonstrate that their cybersecurity systems are equipped against attacks. Private and public companies will be evaluated by regulators who will perform vetting the company's infrastructures and structure, a fine will be issued for whoever companies failed. Ciaran Martine of UK National Cyber Security Centre Stated "Network and information systems give critical support to everyday activities, so it is absolutely vital that they are as secure as possible".

8. CONCLUSION

- Accessibility to ships posses the front line to cyber security, accessibility can be through crewmembers or maintenance personnel or any other intruder who may got a pass to access the ship, in the case of autonomous ship, this will be limited to a high degree, it can be at:

o Stage of building this can be eliminated by proper screening of all equipment by makers prior to delivery.

o Stage of operation, comprises two ways, during regular maintenance, where maintenance personnel will pass through security check and credentials verification by maker and security staff at port. Another during sailing, where all personnel of RCC will pass through security screening and regular back ground check by company security personnel.

o Stage during sailing, where IT personnel will monitor and control flow of data to and from the ship and running security screening of all data.

- The autonomous ship does not pose a prime target, because does not have a crew so no ransom can be fixed, cannot hide or sell the cargo onboard easily without being tracked or confiscated, but might only be used as a tool for further action, which a large effort and also can be easily detected by RCC, if on guard all the time. So the only threat will be to hack into the RCC.

- Most of the accident in the maritime field was related to cyber attack to shore side not onboard, the only cases related to accident involving ships was done for test, experimental and none disclosed. Mainly was suspected to involve organizations suspected to be connected to governments.

- If the act is connected to organization connected to governments then the regulatory framework will require a more involvement on governmental level, which will need an act more binding and obligatory than rules and regulations, it requires a more fundamental action like a treaty, since it is affecting a national security of nations and have a severe economic and safety impacts. IMO as a specialized organization will not be able to form a treaty, the act is required by a higher level such as UN to involve governments at the highest level.

REFERENCES

[1] Allianz Global Corporate and Specialty SE, "Safety and shipping review2016," Allianz Global Corporate and Specialty, 2016.

[2] BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF, IUMI, The Guidelines on Cyber Security Onboard Ships, Ver. 2.0, 2017, 51 p. Available: http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=14

[3] Bob Brewin, 2013. University of Texas Team Hijacks $80 Million Yacht With Cheap GPS Spoofing Gear. Nextgov. Available at https://www.nextgov.com/defense/whats-brewin/2013/07/university-texas-team-hijacks-80-million-yacht-cheap-gps-spoofing-gear/67625/

[4] Danny Palmer, 2017. Petya ransomware: Cyberattack costs could hit $300m for shipping giant Maersk. ZDNet. Available at https://www.zdnet.com/article/petya-ransomware-cyber-attack-costs-could-hit-300m-for-shipping-giant-maersk/

[5] David Hambling, 2017. Ships fooled in GPS spoofing attack suggest Russian cyberweapon. NewScientist. Available at https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/

[6] Jennifer Johnson, 2018. Ports of Barcelona and San Diego hit by cyber attacks. Imarest. Available at https://www.imarest.org/themarineprofessional/item/4473-ports-of-barcelona-and-san-diego-hit-by-cyber-attacks

[7] Julian Ryall, 2016, North Korea interfering with GPS signals in South Korea as China relations deteriorate. The Telegraph. Available at https://www.telegraph.co.uk/news/2016/04/01/north-korea-interfering-with-gps-signals-in-south-korea-as-china/

[8] K. Jones, K. Tam, and M. Papadaki, 2016. "Threats and impacts in maritimecyber security," IET Engineering & Technology Reference.

[9] Pierluigi Paganini, 2018. Ransomware attack disrupted some systems of the shipping giant COSCO in the US. Security Affair. Available at https://securityaffairs.co/wordpress/74779/malware/cosco-ransomware-attack.html

[10] Rothblum A (2000), Human error and marine safety. International Workshop on Human Factors in Offshore Operations (HFW2002)

[11] Simon Hansman, Ray Hunt, 2004. A taxonomy of network and computer attacks, Computers & Security.

[12] T. Peltier, 2005. Information security risk analysis. 2nd. edition Auerbach Publications, available at https://www.taylorfrancis.com/books/9781420031195

[13] Tucci, A.E., 2017. Cyber Risks in the Marine Transportation System. In Cyber-Physical Security (pp. 113-131). Springer International Publishing.